

AO 106 (Rev. 04/10) Application for a Search Warrant

United States District Court
for the
Western District of New York



In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address.)

1010 Cleveland Drive, Cheektowaga, New York 14225 and the person of John Stuart
(Date of Birth 6/1/1998) if found therein

1948 0972

Case No. 20-MJ- 5207

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, which is attached hereto and incorporated by reference herein.

Located in the Western District of New York, there is now concealed (identify the person or describe the property to be seized):
Evidence, fruits and instrumentalities pertaining to violations of Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2), as more fully set forth in Attachment B, which is attached hereto and incorporated by reference herein.

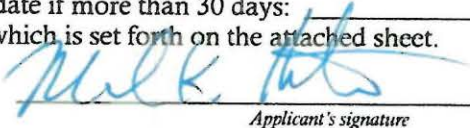
The basis for search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2).

The application is based on these facts:

- ☒ continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

MICHAEL HOCKWATER
TASK FORCE OFFICER
FEDERAL BUREAU OF INVESTIGATION
Printed name and title

Sworn to me and signed telephonically.

Date: October 8, 2020


Judge's signature

City and state: Buffalo, New York

HONORABLE MICHAEL J. ROEMER
UNITED STATES MAGISTRATE JUDGE
Printed name and Title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

STATE OF NEW YORK)
COUNTY OF ERIE) SS:
CITY OF BUFFALO)

I, **MICHAEL HOCKWATER**, a Task Force Officer with the Federal Bureau of Investigation being duly sworn, deposes and states as follows:

INTRODUCTION

1. I am a Police Detective with the Town of Cheektowaga, New York Police Department. I have been a Police Officer since August of 1989. I am currently assigned as a Task Force Officer with the Federal Bureau of Investigation (FBI), Buffalo Field Office, Cyber Task Force, Innocent Images National Initiative, which targets individuals involved in the on line sexual exploitation of children. I have been a Task Force Officer since June 14, 2010. As part of these duties, I have become involved in the investigation of suspected violations of Title 18, United States Code, Sections 2251, 2252, 2252A, 2422, and 2423. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography in various forms of media, including computer media. Moreover, I was deputized as a federal law enforcement officer who is authorized to investigate violations of criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A.

2. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in **Attachment A** of this Affidavit, including the entire property located at **1010 Cleveland Drive, Cheektowaga, NY 14225 (the "SUBJECT PREMISES")**, the content of electronic storage devices located therein, and any person located at the SUBJECT PREMISES, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § Section 2252A(a)(5)(B) and (b)(2) Possession of Child Pornography: which items are more specifically described in **Attachment B** of this Affidavit.

3. The statements contained in this affidavit are based in part on information provided by U.S. federal law enforcement agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies, information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals; and my experience, training and background as an FBI task Force Officer. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) and (b)(1) (receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. § 2252(a)(4)(B)

and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt or distribution of child pornography); and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography) are presently located at the SUBJECT PREMISES.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following: 18 U.S.C. § 2252(a)(2) and (b)(1) (receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. § 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt or distribution of child pornography); and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography)

a. 18 U.S.C. § 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. 18 U.S.C. § 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

c. 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

d. 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or

transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

5. The following terminology pertinent to this investigation is used with the meanings defined below.

a. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the users who sent/received such a message, or by the bulletin board administrator.

b. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles

an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. “Chat room,” as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

d. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

e. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

f. “Cloud storage,” as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user’s computer or other local storage device) and is made available to users over a network, typically the Internet.

g. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

h. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, “thumb,” “jump,” or “flash” drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

i. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set

security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

j. The “Domain Name System” or “DNS” is system that translates readable Internet domain names such as www.justice.gov into the numerical IP addresses of the computer server that hosts the website.

k. “Encryption” is the process of converting data into a code in order to prevent unauthorized access to the data.

l. A “hidden service,” also known as an “onion service,” is website or other web service that is accessible only to users operating within the Tor anonymity network.

m. “Hyperlink” refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

n. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

o. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

p. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (“ISPs”) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

q. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

r. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

s. “Remote computing service,” as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

t. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation;

(d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

u. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, “thumb,” “jump,” or “flash” drives, CD-ROMs, and other magnetic or optical media.

v. The “Tor network” is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a “circuit.”

w. “URL” is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

x. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

y. A “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

6. A user of the Internet account at the SUBJECT PREMISES has been linked to an online community of individuals who regularly send and receive child pornography via a hidden service website that operated on the Tor anonymity network. The website is described below and referred to herein as the "TARGET WEBSITE."¹ There is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES accessed the TARGET WEBSITE, as further described herein.

The Tor Network

7. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are uniquely identified by IP addresses, which are used to route information between Internet-connected devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. On the Internet, data transferred between devices is split into discrete packets, each of which has two parts: a header with non-content routing and control information, such as the packet's source and destination IP addresses; and a payload, which generally contains user data or the content of a communication.

¹ The name of the TARGET WEBSITE is known to law enforcement. Investigation into the users of the website remains ongoing and disclosure of the name of the website would potentially alert active website users to the investigation, potentially provoking users to notify other users of law enforcement action, flee, and/or destroy evidence.

8. The website further described below operated on the Tor network, which is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a “circuit.” Because of the way the Tor network routes communications through the relay computers, traditional IP address-based identification techniques are not effective.

9. To access the Tor network, a user must install Tor software. That is most easily done by downloading the free “Tor browser” from the Tor Project, the private entity that maintains the Tor network, via their website at www.torproject.org.² The Tor browser is a web browser that is configured to route a user’s Internet traffic through the Tor network.

10. As with other Internet communications, a Tor user’s communications are split into packets containing header information and a payload, and are routed using IP addresses. In order for a Tor user’s communications to be routed through the Tor network, a Tor user necessarily (and voluntarily) shares the user’s IP address with Tor network relay computers, which are called “nodes.” This routing information is stored in the header portion of the packet. As the packets travel through the Tor network, each node is able to see the address information of the previous node the communication came from and the next node the

² Tor users may also choose to manually configure a web browser or other application to route communications through the Tor network.

information should be sent to. Those Tor nodes are operated by volunteers – individuals or entities who have donated computers or computing power to the Tor network in order for it to operate.

11. Tor may be used to access open-Internet websites like www.justice.gov. Because a Tor user's communications are routed through multiple nodes before reaching their destination, when a Tor user accesses such an Internet website, only the IP address of the last relay computer (the "exit node"), as opposed to the Tor user's actual IP address, appears on that website's IP address log. In addition, the content of a Tor user's communications are encrypted while the communication passes through the Tor network. That can prevent the operator of a Tor node from observing the content (but not the routing information) of other Tor users' communications.

12. The Tor Project maintains a publicly available frequently asked questions (FAQ) page, accessible from its website, with information about the Tor network. Within those FAQ, the Tor Project advises Tor users that the first Tor relay to which a user connects can see the Tor user's actual IP address. In addition, the FAQ also cautions Tor users that the use of the Tor network does not render a user's communications totally anonymous. For example, in the Tor Project's FAQ, the question "So I'm totally anonymous if I use Tor?" is asked, to which the response is, in bold text, "No."

13. The Tor Network also makes it possible for users to operate or access websites that are accessible only to users operating within the Tor network. Such websites are called “hidden services” or “onion services.” They operate in a manner that attempts to conceal the true IP address of the computer hosting the website. Like other websites, hidden services are hosted on computer servers that communicate through IP addresses. However, hidden services have unique technical features that attempt to conceal the computer server’s location.

14. Unlike standard Internet websites, a Tor-based web address is comprised of a series of either 16 or 56 algorithm-generated characters, for example “asdlk8fs9dfiku7f,” followed by the suffix “.onion.” Ordinarily, investigators can determine the IP address of the computer server hosting a website (such as www.justice.gov) by simply looking it up on a publicly available Domain Name System (“DNS”) listing. Unlike ordinary Internet websites, however, there is no publicly available DNS listing through which one can query the IP address of a computer server that hosts a Tor hidden service. So, while law enforcement agents can often view and access hidden services that are facilitating illegal activity, they cannot determine the IP address of a Tor hidden service computer server via public lookups. Additionally, as with all Tor communications, communications between users’ computers and a Tor hidden service webserver are routed through a series of intermediary computers. Accordingly, neither law enforcement nor hidden-service users can use public lookups or ordinary investigative means to determine the true IP address – and therefore the location – of a computer server that hosts a hidden service.

Description of TARGET WEBSITE

15. The “TARGET WEBSITE” was a child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children that operated from approximately October 2016 to June 2019. In June of 2019, the computer server hosting the TARGET WEBSITE, which was located outside of the United States, was seized by a foreign law enforcement agency.

16. While it operated, the website administrator posted a message on the website describing its purpose as being to “share cp of babies and toddlers.” The term “cp” in this context refers to child pornography. The name of the TARGET WEBSITE contained a reference to children of that age and the website logo included images depicting babies and toddlers. The TARGET WEBSITE name itself is a reference to the genitalia of prepubescent boys. The TARGET WEBSITE allowed users to make and view postings that contained text, still images, video images, and/or web links that directed members to specific content located on another website. The TARGET WEBSITE also had a private message feature that allowed users to send private messages to each other.

17. The TARGET WEBSITE also had a separate, selective membership section that provided such members with exclusive child pornographic content. To join that selective membership, members were required to upload nude or sexually explicit images depicting babies and toddlers. As of June 2019, the website had over 230,000 members and over 29,000

postings. While it operated, FBI Special Agents accessed the TARGET WEBSITE and downloaded digital child pornography content accessible via the website, in an undercover capacity.

18. Upon accessing the TARGET WEBSITE, the initial web page revealed a message board including links a user would access to register and log-in, as well as hyperlinked message board headings titled, "Announcements," "Rules," "Allowed Hosts," "How to post," "Security," and "Apply for VIP." Upon accessing the "Apply for VIP" hyperlink on the TARGET WEBSITE, users would observe the following text:

Forum Rules, Application for VIP:

- Only child porn (nude or sex) pics or videos of babies and toddler
- All archives must be encrypted in Rar or 7Zip format
- The archive passwords must contain your nickname and [TARGET WEBSITE name]
- Don't forget provide a live preview
- Only use safe hosts without javascript
- No need to apply with private stuff. Random CP of 0-5yo is accepted (boys and girls).

19. Based upon my training and experience, I am aware that "Rar" and "7Zip" refer to archive files, which are a method of storing multiple digital files (image or videos for example) in a single, compressed file, which may be password-protected; that a "live preview"

consists of a representative sub-set of a set of still images or still shots from a video, which give a user a preview of the full image set or video available for download; and a “safe host” refers to a file hosting provider on whose servers password-protected digital files may be stored, which is perceived by users of the website to not be compliant with law enforcement requests for information.

20. Upon accessing the “Register” link of the TARGET WEBSITE, users completed a “Username,” and “Password,” field, as well as a “Confirmation” code to enter the website. Located at the bottom of the web page are two additional sections entitled “The Team” and “Delete All board cookies.” “The Team” section listed the usernames of three website “Administrators.”

21. After successfully registering, a user was taken to a web page stating that an account has been created and the user may login with username and password. A user was then able to access the “Board Index.” Sections for posting to the website within the Board Index included: “CP Stars,” with forums “Boys” and “Girls;” “Babies (0-1YO),” with forums “Baby Boys” and “Baby Girls;” and “Toddlers (2-5YO),” with forums “Toddler Boys” and “Toddler Girls.”

22. Upon accessing a user posting on the website, the original post appeared at the top of the page, with any corresponding replies to the original post included in the thread below it. Typical posts contained text, images, links to external sites, or replies to previous

posts. A review of postings within these sections revealed numerous posts containing images depicting child pornography and child erotica of prepubescent males, females, toddlers, and infants. Examples of these are as follows:

a. On May 14, 2017, a website administrator posted a topic entitled “We are back” in the “Announcements” forum that contained the following statement: “Only CP contributors will have access now to the stuff. If you are not VIP, make your application for member...” The post contained an image depicting a prepubescent male, who appeared naked below the waist exposing his genitals, and featured a green post it note reading, “May-13-2017” along with what appeared to be the username of another website administrator. Among other things, the image focused on the exposed penis of the prepubescent male. Based upon my training and experience, the significance of this posting was to effectively make membership available only to those users who uploaded child pornography to the website.

b. On May 23, 2017, a website administrator posted a message entitled “Inactive” in the “Announcements” forum that contained the following: “Abandoned accounts was automated deactivated. VIP accounts will be also automated deactivated after 2 months, if they not make any contribution.” Based on my training and experience, a “contribution” means a posting to the website, generally one that contains or provides a link to child pornography images/videos. Below the text of the post, a photo of a prepubescent female child with her legs spread, focusing on her vagina, was displayed. In the top left of the photo were textual graphics that included what appeared to be usernames of website users and administrators as well as the term “1yo,” and a torn green post-it note that read, “[TARGET

WEBSITE name],” contained the web address for TARGET WEBSITE, and the text “Exclusive 0-5yo NEW 2017.”

c. On June 30, 2017, a review of the website revealed a post from a website member titled “Toddler Fuck” in the “Toddlers (2-5yo)” forum. The post contained an image depicting a prepubescent male toddler, appearing naked and exposing his genitals, on his back while an adult male penis entered his anus. The image focused on the exposed adult male penis penetrating the toddler.

Evidence Related to Identification of Target that Accessed TARGET WEBSITE

23. I am aware that U.S. as well as foreign law enforcement agencies investigate anonymous offenders engaging in online child sexual exploitation via Tor hidden service websites such as the website(s) described herein. Those websites are globally accessible. The websites and their users may therefore be located anywhere in the world. Due to the anonymity provided by the Tor network, it can be difficult or impossible to determine, at the beginning of an investigation, where in the world a particular website or user is located. Accordingly, when a law enforcement agency obtains evidence that such a website or website user may be located in another country, it is common practice for that law enforcement agency to share information with a law enforcement agency in the country where the website is located or the offender appears to reside, in accordance with each country’s laws.

24. In August 2019, a foreign law enforcement agency (referenced herein as “FLA”) known to the FBI and with a history of providing reliable, accurate information in

the past, notified the FBI that FLA determined that on May 28, 2019, IP address 74.77.4.235 “was used to access online child sexual abuse and exploitation material” via a website that the FLA named and described as the TARGET WEBSITE.

25. FLA described the website as having “an explicit focus on the facilitation of sharing child abuse material (images, links and videos), emphasis on babies and toddlers (ages 0-5 years old),” stated that “[u]sers were required to create an account (username and password) in order to access the majority of the site and hosted material,” and provided further documentation naming the site as the TARGET WEBSITE, which the FLA referred to by its actual name.

26. FLA is a national law enforcement agency of a country with an established rule of law. There is a long history of U.S. law enforcement sharing criminal investigative information with FLA and FLA sharing criminal investigative information with U.S. law enforcement, across disciplines and including the investigation of crimes against children. FLA advised U.S. law enforcement that it obtained that information through independent investigation that was lawfully authorized in FLA’s country pursuant to its national laws. FLA further advised U.S. law enforcement that FLA had not interfered with, accessed, searched or seized any data from any computer in the United States in order to obtain that IP address information. U.S. law enforcement personnel did not participate in the investigative work through which FLA identified the IP address information provided by FLA.

27. I am aware through my training and experience and consultation with other U.S. law enforcement agents that tips provided by FLA regarding IP addresses that FLA advised were associated with access to Tor network child exploitation-related web and chat sites have: (1) led to the identification and arrest of a U.S.-based child pornography producer and hands-on offender, and the identification and rescue of multiple U.S. children subject to that offender's ongoing abuse; (2) led to the seizure of evidence of child pornography trafficking and possession; and (3) been determined through further investigation to be related to targets that U.S. law enforcement investigation had independently determined were associated with child pornography trafficking and possession.

28. As described herein, the TARGET WEBSITE could not generally be accessed through the traditional internet. Only a user who had installed the appropriate Tor software on the user's computer could access the "TARGET WEBSITE." Even after connecting to the Tor network, however, a user would have to find the 16-or-56-character web address of the TARGET WEBSITE in order to access it. Hidden service websites on the Tor Network are not "indexed" by search engines—such as Google—to anywhere near the same degree as websites that operate on the open Internet. Accordingly, it is much more difficult to perform a Google-type search of hidden service websites than it is to search open Internet websites for particular content of interest. Users interested in accessing child exploitation material (or in advertising child exploitation and pornography websites they operate) therefore keep, maintain and use directory sites that advertise the web addresses of hidden services that contain child exploitation related content. Those directory sites also operate via the Tor

network. Users utilize those directory sites to identify new web forums, chat sites, image galleries and file hosts pertaining to the sexual exploitation of children. Such directory sites often identify whether particular sites are then operating, whether child pornography imagery may be found there, and even what types of child pornography are accessible (i.e., boys, girls, or “hurtcore”). They also contain clickable hyperlinks to access those sites. As with other hidden service websites, a user must find the 16-or-56 character web address for a directory website in order to access it. While it operated, the web address for the website described herein was listed on one or more of such directory sites advertising hidden services dedicated to the sexual exploitation of children.

29. I am also aware through consultation with FBI agents that the review of detailed user data related to one Tor network based child pornography website found that it was exceedingly rare for a registered website user to access that website and never return. FBI review of user data from that website found that less than two hundredths of one percent of user accounts registered an account on the website, accessed a message thread on the website, and then never returned to the website and logged in to the same account.

30. Accordingly, based on my training and experience and the information articulated herein, because accessing the TARGET WEBSITE required numerous affirmative steps by the user – to include downloading Tor software, accessing the Tor network, finding the web address for TARGET WEBSITE, and then connecting to TARGET WEBSITE via

Tor – it is extremely unlikely that any user could simply stumble upon TARGET WEBSITE without understanding its purpose and content.

31. Accordingly, I submit that there is probable cause to believe that, for all of the reasons described herein, any user who accessed the TARGET WEBSITE has, at a minimum, knowingly accessed the TARGET WEBSITE with intent to view child pornography, or attempted to do so.

Identification of SUBJECT PREMISES

32. According to publicly available information, IP address 74.77.4.235 which was used to access TARGET WEBSITE on **May 28, 2019** was registered to Charter Communications.

33. On November 20, 2019, a subpoena/summons was issued to Charter Communications in regard to the pertinent IP address. A review of the results obtained on June 18, 2020 identified the following account holder and address, which is the address of the SUBJECT PREMISES: John Stuart, 1010 Cleveland Drive, Cheektowaga, NY 14225, telephone (716) 870-1014, email address johnms88@gmail.com..

34. A search of a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, and other information was conducted for John Stuart. These public records indicated that John Stuart's current address

is 1010 Cleveland Drive, Cheektowaga, NY 14225. A check with the Department of Motor Vehicles on or about July 14, 2020, revealed that an individual named John Stuart with a date of birth of 6/01/1988 resides at the SUBJECT PREMISES.

35. On or about July 24, 2020 I conducted Surveillance of the SUBJECT PREMISES and observed a male matching the description of John Stuart exited a vehicle parked in the driveway and enter the rear door of the residence. The vehicle registered to John Stuart was observed parked in the driveway of the SUBJECT PREMISES on occasions between July 24, 2020 and July 29, 2020.

36. On or about July 24, 2020, I also conducted a check of the wireless networks in the immediate area of the SUBJECT PREMISES. There were multiple wireless networks observed in the area but all of them were secured.

37. A check of open source information from the Internet regarding John Stuart revealed that he is a paramedic with a private ambulance service in western New York.

**Pen Register and Trap and Trace on
Residential Internet Service for SUBJECT PREMISES**

38. On August 18, 2020, the United States Magistrate Judge Jeremiah J. McCarthy authorized the installation and use of a pen register/trap and trace device (PRTT) to record, decode and/or capture all dialing, routing addressing and signaling information associated

with each communication to or from the residential internet service account associated with the SUBJECT PREMISES provided by Charter Communications (20-MR-257). Based on my training and experience, I am aware that analysis of data obtained via a PRTT on a target's residential internet connection can provide evidence that a user of the internet at the premises is accessing the Tor network. That is possible because the IP addresses of Tor node computers that make up the network are published by the Tor network. Since a residential internet PRTT will disclose the IP addresses of computers and electronic devices to which communications are sent and from which communications are received, analysis of the PRTT data can reveal Tor use. Due to Tor routing and encryption, a PRTT will not reveal the ultimate destination or the content of those communications. Charter Communications began to provide data pursuant to the Court's order on August 20, 2020. Analysis through October 6, 2020 of the data provided pursuant to that PRTT order revealed evidence that a user of the internet at the SUBJECT PREMISES accessed the Tor network on fourteen separate days since the start of the data being provided; on August 23, August 29, September 5, September 6, September 11, September 13, September 14, September 18, September 19, September 25, September 30, October 2, October 5 and October 6, 2020.

39. Based on my training and experience, although the TARGET WEBSITE is no longer in service, the fact that an internet user at the SUBJECT PREMISES continue to access the Tor network means that it is likely the user is continuing to use the Tor network for child exploitation purposes. While I know that the Tor network contains sites other than those involving child pornography, I know based on my training and experience that the Tor

network contains many sites dedicated to child pornography and child exploitation, just like the TARGET WEBSITE, and individuals that seek out child pornography will continue to do so even if a website they have utilized in the past is no longer in service.

**BACKGROUND ON CHILD PORNOGRAPHY,
COMPUTERS, AND THE INTERNET**

40. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the

world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as “apps.” Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one’s favorite websites in, for example, “bookmarked” files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user’s Internet activities generally leave traces or “footprints” in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

41. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who access online child sexual abuse and exploitation material via a website:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction

from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain child pornographic material in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain those materials and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.³

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain contact information (e.g. online messaging accounts, email addresses, etc.) of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Even if the target uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

³ See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

42. Based on all of the information contained herein, I believe that an internet user residing at the SUBJECT PREMISES likely displays characteristics common to individuals who access online child sexual abuse and exploitation material via a website. In particular, the target of investigation obtained and used Tor network software, found the web address for TARGET WEBSITE, and accessed online child sexual abuse and exploitation material via the TARGET WEBSITE.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

43. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

44. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active

file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

45. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on

the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can

indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under investigation. For example, information within the computer may indicate

the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for

committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

46. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search website all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial

amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

47. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

48. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that

reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

49. This warrant permits law enforcement to compel John Stuart and any other individual present at the time of the execution of the search warrant to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to

the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from

other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any DEVICES that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of John Stuart and any other individual present at the time of the execution of the search warrant to the fingerprint scanner of the DEVICES found at the PREMISES; (2) hold the DEVICES found at the PREMISES in front of the face of John Stuart and any other individual present at the time of the execution of the search warrant and activate the facial recognition feature; and/or (3) hold the DEVICES found at the PREMISES in front of the face of John Stuart and any other individual present at the time of the execution of the search warrant and activate the iris recognition feature, for the purpose of attempting to unlock the DEVICES in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel that John Stuart and any other individual present at the time of the execution of the search warrant state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to compel John Stuart and any other individual present at the time of the execution of the search warrant to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

CONCLUSION

50. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

52. In addition, it is and has been the standard and ordinary practice of FBI that during the execution of search warrants, Special Agents take entry and exit photographs of the premises to be searched, as well as photographs of the specific places in which items are found and from which items are seized. The purpose of this procedure is to preserve an accurate record of the condition and appearance of the premises upon the arrival and exit of the search team, and to preserve an accurate record of the locations within the premises where items are found and from which such items are seized.

SEALING REQUEST

53. Finally, since this affidavit relates to an ongoing criminal investigation and contains the names of individuals who are witnesses and/or targets in this matter, the government respectfully moves this Court to issue an Order sealing until further order of the Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the required inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left at the premises to be searched).



MICHAEL HOCKWATER
Federal Bureau of Investigation
Task Force Officer

Sworn to and subscribed telephonically

this 8th day of October, 2020.



HONORABLE MICHAEL J. ROEMER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The entire property located at **1010 Cleveland Drive, Cheektowaga, New York 14225** including the residential building, any outbuildings, and any appurtenances thereto (the SUBJECT PREMISES, further described as follows: a two story residence, white in color with a detached two car garage located on the north side of the street. The number "1010" is affixed to the front of the residence.



And the person of the following individual if he is present at the SUBJECT PREMISES at the time of the search warrant's execution:



John Stuart
Date of birth: June 1, 1998.

ATTACHMENT B

ITEMS TO BE SEARCHED FOR AND SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. § Section 2252A(a)(5)(B) and (b)(2) Possession of Child Pornography, to be searched for and seized from the location and/or person to be searched as described in **Attachment A**:

1. Computers, storage media, and any and all cellular phones that reasonably appear to be under the custody or control of JOHN STUART (hereinafter, "DEVICES").
2. On any DEVICE whose seizure is otherwise authorized by this warrant:
 - a. all visual depictions, including still images, videos, films or other recordings, in whatever form, of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, or engaged in sexually suggestive conduct (such as exposing and/ or touching their breasts or genitalia), and any mechanism used for the production, receipt, distribution, advertisement, or storage of the same;
 - b. any and all documents, records, images, videos, emails, email software, associated email addresses, email address book contents, internet history, browsing history, internet search history, cookies, deleted files, bookmarked and favorite web pages, user typed web addresses, desktop shortcuts, path and file names for files opened through any media and/or image viewing software, chat software, chat applications, chat files, chat logs, chat names used, peer to peer software, peer to peer files, newsgroup postings by the user, IP addresses assigned, and other evidence pertaining to the receipt, distribution, transmission, and possession of child pornography;

- c. any and all records, documents, programs, applications, or materials, including electronic mail and electronic messages, pertaining to or constituting communications with any individuals believed to be under the age of 18
- d. evidence of who used, owned, or controlled the DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- e. evidence of software that would allow others to control the DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- f. evidence of the lack of such malicious software;
- g. evidence indicating how and when the DEVICE was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;
- h. evidence indicating the DEVICE user's knowledge and/or intent as it relates to the crime(s) under investigation;
- i. evidence of the attachment to the DEVICE of other storage devices or similar containers for electronic evidence;
- j. evidence of programs (and associated data) that are designed to eliminate data from the DEVICE;
- k. evidence of the times the DEVICE was used;
- l. passwords, encryption keys, and other access devices that may be necessary to access the DEVICE or other seized DEVICES;
- m. documentation and manuals that may be necessary to access the DEVICE or to conduct a forensic examination of the DEVICE;
- n. records of or information about Internet Protocol addresses used by the DEVICE;

- records of or information about the DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
 - p. contextual information necessary to understand the evidence described in this attachment.
- Routers, modems, and network equipment used to connect computers to the Internet.
- Entry and exit photographs of the premises to be searched, as well as photographs of the specific places in which items are found and from which items are seized
- Records, information, and items relating to violations of the statutes described above including:
 - a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, 1010 Cleveland Drive, Cheektowaga, New York 14225 including utility and telephone bills, mail envelopes, or addressed correspondence;
 - b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
 - c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;
 - d. Records and information relating to sexual exploitation of children, including correspondence and communications between users of child pornography and exploitation websites.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to compel all individuals present at the SUBJECT PREMISES to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

- (a) any of the DEVICES found at the PREMISES, and
- (b) where the DEVICES are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the DEVICES's security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the PREMISES to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any DEVICE. Further, this warrant does not authorize law enforcement personnel to request that John Stuart state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete

copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.